RES212 Example of Exam

25/6/2018

Firstname		LASTNAME	
Cycle/ID		QCM No.	0

Instructions :

— You must return ALL paper sheets : any non-complete copy will have a 0/20 score.

— Do not forget to fill your personal details above

— This exam has multiple-choice questions (QCM) on course and labs topics.

— Each QCM question has *a single correct answer* : notice that while most wrong answers have a null score, some answers to few QCM questions might have a *negative score*.

— You have to report ALL your answers in the table above (as a single UPPERCASE letter). Only answers in the table will be counted for the final score.

Question	1	2	3	4	5	6	7	8	9	10	11	12	13
Answer													
Question	14	15	16	17	18	19	20	21	22	23	24	25	
Answer													

Question 1. IPsec is a family of security protocols with different modes of operation (i.e., gateway-to-gateway tunnel ; end-to-end transport) proposing multiple security services (e.g., data origin authentication ; traffic confidentiality ; traffic flow confidentiality).

A) True

B) False

Question 2. Honeypot is an active attack

A) False

B) True

Question 3. "Digital signature" is a security mechanism that can be used to provide a "data origin authentication" service

A) True

B) False

Question 4. Virtual private networks (VPNs) can be realized with technologies such as GRE/PPTP tunnels (L2), IPsec (L3) TLS and SSH (L4 and above)

A) True

B) False

Question 5. Encryption and digital signatures are among the main security services

A) True

B) False

Question 6. The Transport Layer Security (TLS) record protocol computes the Message Authentication Code (MAC) over :

A) transmitted encrypted data, transmitted record header, non-transmitted sequence number

B) transmitted unencrypted data, transmitted record header, non-transmitted sequence number

C) transmitted encrypted data, transmitted record header, transmitted sequence number

D) transmitted unencrypted data, transmitted record header, transmitted sequence number

Question 7. In computer security, an ingress firewall is used to typically check compliance of user traffic with some policy

A) False

B) True

Question 8. Firewalls can perform different operations on the screened traffic. An *application gateway* normally performs : flow tracking, L7 payload parsing, state machine reconstruction ;

A) False

B) True

Question 9. The IPsec Encapsulated Security Payload (ESP) protocol, in addition to the services offered by the IPsec Authentication Header (AH) protocol, offers

A) Traffic flow confidentiality only

B) Data confidentiality only integrity

C) Data and Traffic flow confidentiality

Question 10. In iptables/netfilter, when packets trigger conditions that yield to a `ACCEPT` action, one must still take care that the traffic in the *reverse direction* is properly handled (e.g., using the circuit-level logic provided by the `state` or `conntrack` modules)

A) False

B) True

Question 11. A hash function has a variable-length input and a fixed-length output

A) True

B) False

Question 12. Security attacks can be broadly characterized as either passive or active attacks

A) True

B) False

Question 13. Network intrusion prevention sytems (NIPS) complement the operation of Network intrusion detection sytems (NIDS) by providing fast and fully automated response to alerts generated by the latter

A) False

B) True

Question 14. Public Key Infrastructures (PKI) are used to distribute and verify X.509 certificates, and have no known cryptographic or protocol weaknesses

A) True

B) False

Question 15. iptables/netfilter are respectively a Linux kernel module and a user-space firewall application used to configure iptables kernel hooks

A) False

B) True

Question 16. Multi-protocol Label Switching (MPLS) is a technology that ISPs can use to implement Virtual Private Network (VPNs), that helps in switching and isolating traffic of different VPNs

A) True

B) False

Question 17. In IPsec, the parameters of the Security Association (SA) negociated via the Internet Key Exchange (IKEv2) protocol

A) are proposed as a list by the initiator, and are ultimately selected by the responder

B) are proposed as a list by the responder, and are ultimately selected by the initiator

Question 18. When in transport mode, the IPsec Encapsulated Security Payload (ESP) header and ESP authentication trailer encapsulate :

A) the transport (TCP/UDP/etc.) and payload data (plus optionally a padding trailer) of the non-encrypted packet

B) the original network header (IP), transport header (TCP/UDP/etc.) and payload data (plus optionally a padding trailer) of the non-encrypted packet

C) the transport header (TCP/UDP/etc.) and payload data (plus optionally a padding trailer) of the encrypted packet

D) the original network header (IP), transport header (TCP/UDP/etc.) and payload data (plus optionally a padding trailer) of the encrypted packet

Question 19. Output FeedBack (OFB) mode is a mode of operation of block ciphers that offers confidentiality, and its use can still be recommended today, since (with proper initialization) it is still cryptographically safe

A) False

B) True

Question 20. The Transport Layer Security (TLS) handshake message sequence comprises 4 phases : in case of an *abbreviated exchange* to refresh the key material, some of these phases can be skipped

A) True

B) False

Question 21. The Transport Layer Security (TLS) protocol is immune to the SSL/STARTTLS stripping attacks provided that a HTTP Strict Transport Security (HSTS) header is present in the first connection to a domain

A) False

B) True

Question 22. X.509 certificates contain, among other fields, the Certification Authority (CA) identity, the User identity and public key, a cryptographic digest of all the certificate, and finally the same digest encrypted with the CA private key

A) False

B) True

Question 23. Authentication, access control, data confidentiality and non repudiation are among the main security mechanisms

A) False

B) True

Question 24. One of the primary goals of asymmetric key cryptography is to digitally signs objects (providing authentication, integrity protection and non-repudiation)

A) False

B) True

Question 25. The Transport Layer Security (TLS) handshake message sequence comprises 4 phases : in the 1st phase, the client selects one among the cipher algorithms proposed by the server

A) True

B) False